19.

Die Ringe mit lauter isomorphen nichttrivialen endlich erzeugbaren Unterringen

Von F. SZÁSZ in Budapest

Professor L. Rédei zum 60. Geburtstag gewidmet

Ein Ring A wird ein Ω-Ring genannt, wenn die nichttrivialen (d. h. von A und von O verschiedenen) endlich erzeugbaren Unterringe von A untereinander isomorph sind. Unser Zweck ist die sämtlichen Ω-Ringe zu bestimmen. Die Ringe A ohne nichttriviale Unterringe, also die Ringe A mit $|A|=p$ oder 1 sind ebenfalls als Ω-Ringe anzusehen, wobei $|A|$ die Mächtigkeit von A und p eine Primzahl bezeichnet. I bezeichnet den Ring der ganzen rationalen Zahlen. Bezüglich der nötigen Grundbegriffe der Algebra verweisen wir auf die Lehrbücher [1], [2] und [3].

Rédei und Szele [4] haben die Ringe mit torsionsfreier additiver Gruppe ersten Ranges bestimmt. Insbesondere werden wir gewinnen, daß die unendlichen Ω-Ringe mit den torsionsfreien Zeroringen ersten Ranges übereinstimmen.

Wir werden später die folgenden drei elementaren Vorbemerkungen oft berücksichtigen:

1. Jeder Unterring eines Ω-Ringes ist ebenfalls ein Ω-Ring.

2. Jedes Element a von der (additiven) Ordnung $O(a)=n(\in I, \neq 0)$ eines Ω-Ringes A ist die Wurzel eines Polynoms:

$$f(x)\,(\in x(I/(n))[x], \neq 0),$$

denn im entgegengesetzten Fall wären die endlich erzeugten nichttrivialen Unterringe $\{a^2\}$ und $\{a^2, a^3\}$ untereinander nichtisomorph, sogar könnte der zweite nicht durch ein Element erzeugt werden.

3. Jeder endliche nichtnilpotente Ω-Ring A mit der Bedingung $pA=0$ ist halbeinfach, denn ein solcher Ring A besitzt einen Unterring $\{e\}$ mit $e^2=e\neq 0$, woraus folgt, daß A überhaupt keine nilpotenten Elemente $(\neq 0)$ haben kann. Hierbei bezeichnet $\{\ldots, x_\alpha, \ldots\}$ den durch die eingeklammerten Elemente erzeugten Unterring von A.

Es gilt der

S a t z. *Jeder Ω-Ring ist zu einem der folgenden Ringe isomorph:*

1. *die Zeroringe mit torsionsfreier additiver Gruppe ersten Ranges;*
2. *die Ringe mit zyklischer additiver Gruppe von der Ordnung p^2 oder p;*
3. *die direkten Summen $K_p \oplus K_p$ von zwei isomorphen endlichen Primkörpern;*
4. *die endlichen Körper von der Ordnung p^q (p und q sind beliebige Primzahlen);*
5. *die Ringe A mit $A^2 = pA = 0$ und $|A| = p^2$;*
6. *die Ringe $A = \{a\}$ mit den definierenden Gleichungen $pa = a^2 = 0$.*

B e w e i s. Da alle im Satz erwähnten Ringe offenbar Ω-Ringe sind, genügt es zu beweisen, dass jeder Ω-Ring tatsächlich zu einem der erwähnten Ringe isomorph ist. Es sei also A ein beliebiger Ω-Ring.

Wir beweisen, daß die additive Gruppe A^+ eines Ω-Ringes A entweder torsionsfrei oder periodisch ist. Im engegengesetzten Fall gibt es nämlich in A Elemente a und b mit

$$a \neq 0, \ b \neq 0, \ O(a) = n(\neq 0, \in I), \ O(b) = 0,$$

und es gelten $\{mb\} = \{b\} = A$ für jede Zahl m $(\neq 0, \in I)$, da $\{a\}$ und $\{b\}$ nichtisomorph sind. Hiernach ist aber A^+ wegen

$$mA = m\{b\} \supset \{mb\} = A \supset mA$$

offenbar eine vollständige („divisible") Abelsche Gruppe. Also enthält A^+ wegen $O(a) \neq 0$ eine Untergruppe $Z(p^\infty)$. Da jede Untergruppe von $Z(p^\infty)$ auch ein Unterring von A ist, besitzt ein Ω-Ring A gewiß keine Untergruppe $Z(p^\infty)$. Dieser Widerspruch zeigt, daß A^+ entweder torsionsfrei, oder periodisch ist.

Es wird jetzt bewiesen, daß jeder Ω-Ring A mit einer torsionsfreien additiven Gruppe A^+ Nullteiler enthalten soll. Aus der Voraussetzung, daß ein Ω-Ring mit torsionsfreier additiver Gruppe A^+ nullteilerfrei ist, kann nämlich ein Widerspruch folgenderweise abgeleitet werden.

Ist $a \neq 0$ ein beliebiges Element des nullteilerfreien Ω-Ringes A mit einer torsionsfreien additiven Gruppe A^+, so gelten für jedes Minimalpolynom

$$f(x) = n_1 x + n_2 x^2 + \cdots + n_s x^s \qquad (n_i \in I)$$

von a, das wegen der Vorbemerkung 2 gewiß existiert, offenbar $n_1 x \neq 0$ und $n_s x^s \neq 0$, denn A ist jetzt nullteilerfrei. Mit einer Zahl $n_0 (\neq 0, \in I)$ erhält man

$$n_0\{n_s a\} \neq 0, \quad n_0\{n_s a\} \neq \{n_s a\},$$

wobei die Gruppe $\{n_s a\}^+$ wegen

$$(n_s a)^s + n_{s-1}(n_s a)^{s-1} + \cdots + n_s^{s-2} n_1 (n_s a) = 0$$

eine endlich erzeugbare Abelsche Gruppe ist.

Es sei jetzt $b = n_0 n_s a (\neq 0)$ mit einem Minimalpolynom

$$g(x) = m_1 x + \cdots + m_t x^t (m_j \in I,\ m_1 x \neq 0,\ m_t x^t \neq 0).$$

Bezeichnet φ einen Isomorphismus von dem nichttrivialen Unterring $\{b\}$ auf den nichttrivialen Unterring $\{m_1 b\}$ von A, so existiert ein Paar von Polynomen

$$h(x),\ h_1(x) (\in x \cdot I[x],\ \neq 0)$$

mit den Bedingungen

$$b\varphi = h(m_1 b) (\in \{m_1 b\}),\ h(m_1 x) = m_1 h_1(x).$$

Ist ferner $b_1 = h_1(b) (\in \{b\})$, so erhält man offenbar

$$g(m_1 b_1) = g(m_1 h_1(b)) = g(h(m_1 b)) =$$
$$= g(b\varphi) = g(b)\varphi = 0\varphi = 0.$$

Kürzt man aber durch m_1^2 $(\neq 0)$ in der (explizit aufgeschriebenen) Gleichung $g(m_1 b_1) = 0$ ab, was wegen der vorausgesetzten Torsionsfreiheit von A^+ erlaubt ist, so ergibt sich wegen

$$g(x) = m_1 x + \cdots + m_t x^t$$

sofort $b_1 = eb_1 (\neq 0)$ mit der Bezeichnung

$$e = -(m_2 b_1 + m_3 m_1 b_1^2 + \cdots + m_t m_1^{t-2} b_1^{t-1}).$$

Da aber A nach der Voraussetzung nullteilerfrei ist, so ist e wegen $b_1 = eb_1 \neq 0$ das Einselement von A. Dann gilt auch $\{e\} \simeq I$, was wegen Vorbemerkung 1 einen Widerspruch bedeutet, denn I ist offenbar kein Ω-Ring.

Also besitzt jeder Ω-Ring A mit einer torsionsfreien additiven Gruppe A^+ Elemente $y_1 \neq 0$ und $y_2 \neq 0$ mit $y_1 y_2 = 0$. Es wird jetzt $A^2 = 0$ folgenderweise bewiesen. Sind $\{y_1\}$ und $\{y_2\}$ nicht beide nichttriviale Unterringe von A, so können wir von diesen Elementen y_1 und y_2 auf weitere Elemente $z_1 \neq 0$ und $z_2 \neq 0$ mit $z_1 z_2 = 0$ übergehen, mit denen beide Unterringe $\{z_1\}$ und $\{z_2\}$ von A nichttrivial sind. Die Unterringe $\{ky_i\}$ sind nämlich mit einer geeigneten natürlichen Zahl k gewiß nichttrivial. Dann können die additiven Gruppen der Ringe $\{z_i\}$ $(i = 1, 2)$ durch gewisse endliche Systeme von Elementen

$$z_i,\ z_i^2,\ z_i^3, \ldots, z_i^{k_i}$$

erzeugt werden. Daher sind aber wegen $z_1 z_2 = 0$ die endlich vielen Elemente

$$\begin{array}{llllll}
 & z_1, & z_1^2, & z_1^3, \ldots, & & z_1^{k_1} \\
z_2, & z_2 z_1, & z_2 z_1^2, & z_2 z_1^3, \ldots, & & z_2 z_1^{k_1} \\
z_2^2, & z_2^2 z_1, & z_2^2 z_1^2, & z_2^2 z_1^3, \ldots, & & z_2^2 z_1^{k_1} \\
z_2^3, & z_2^3 z_1, & z_2^3 z_1^2, & z_2^3 z_1^3, \ldots, & & z_2^3 z_1^{k_1} \\
\vdots & & & & & \\
z_2^{k_2}, & z_2^{k_2} z_1, & z_2^{k_2} z_1^2, & z_2^{k_2} z_1^3, \ldots, & & z_2^{k_2} z_1^{k_1}
\end{array}$$

die additiven Erzeugenden der Gruppe $\{z_1, z_2\}^+$, die hiernach die direkte Summe von endlich vielen zyklischen Gruppen ist. Wir werden jetzt auf weitere Elemente $r_1 \neq 0$ und $r_2 \neq 0$ mit $\{r_1, r_2\} \neq A$ und $r_1 r_2 = 0$ übergehen. Ist $\{z_1, z_2\} = A$, so ist A^+ die direkte Summe von endlich vielen zyklischen Gruppen, woraus die Existenz einer Zahl $k_0 (\neq 0, \in I)$ mit $k_0 A^+ \neq A^+$ folgt. Dann seien $r_1 = k_0 \cdot z_1$ und $r_2 = k_0 \cdot z_2$. Ist aber $\{z_1, z_2\} \neq A$, so seien $r_1 = z_1$ und $r_2 = z_2$. In beiden Fällen erhält man $\{r_1, r_2\} \neq A$ mit $r_1 \cdot r_2 = 0$, und es wird jetzt $\{r_1, r_2\}^2 = 0$ folgenderweise bewiesen.

Da im Ω-Ring A die additiven Untergruppen $\{r_1\}^+$ von $\{r_1\}$ und $\{r_2\}^+$ von $\{r_2\}$ denselben endlichen (torsionsfreien) Rang besitzen, liegt ein Vielfaches $l r_2 \neq 0 (l \in I)$ von r_2 im Unterring $\{r_1\}$. Hiernach existiert ein Polynom

$$w(x) (\neq 0, \in x \cdot I[x])$$

mit $w(r_1) = l r_2$, woraus wegen $r_1 r_2 = 0$ und $w(r_1) r_2 = 0$ gewiß $l r_2^2 = 0$ folgt. Wegen der Torsionsfreiheit von A^+ und $l \neq 0$ gilt auch $r_2^2 = 0$. Also ist $\{r_2\}^+$ ein Zeroring mit einer unendlichen zyklischen additiven Gruppe. Da hiernach jeder endlich erzeugbare echte Unterring U von A ein zyklischer Zeroring ist, kann man $A^2 = 0$ und Rang $A^+ = 1$ beweisen.

$\{l_0 x\}$ ist nämlich für jedes $x \in A$ mit einer geeigneten Zahl $l_0 (\neq 0, \in I)$ ein echter Unterring von A, und aus $(l_0 x)^2 = 0$ folgt $x^2 = 0$ für jedes x, denn A^+ ist torsionsfrei. Ferner gewinnen wir aus $(x+y)^2 = 0$ gewiß $yx = -xy$ für beliebige $x, y \in A$, woraus folgt, daß $\{x, y\}^+$ die direkte Summe von endlich vielen zyklischen Gruppen ist. Dann existiert eine Zahl $m_0 (\neq 0, \in I)$ mit $\{m_0 x, m_0 y\} \neq A$. Da $\{m_0 x, m_0 y\}$ nach den vorigen ein zyklischer Zeroring ist, erhält man wegen der Torsionsfreiheit tatsächlich $A^2 = 0$ und auch Rang $A^+ = 1$. Also ist A ein Zeroring ersten Ranges.

Nach den vorigen ist die additive Gruppe eines Ω-Ringes A, der ein Element $a \neq 0$ von der additiven Ordnung $O(a) \neq 0$ hat, periodisch. Ist die Ordnung $O(a_0)$ eines Elementes $a_0 \in A$ eine Primzahl p, so ist gewiß $p^2 A^+ = 0$, denn im Falle der Existenz eines Elementes $a_1 \in A$ mit $O(a_1) = p^3$ wären $\{a_1\}$ und $\{p a_1\}$ echte nichtisomorphe Unterringe von A. Also ist A^+ wegen der Definition des Ω-Ringes eine p^2-beschränkte Abelsche p-Gruppe.

Es sei jetzt $A[p]=[x; px=0, x \in A]$. Dann ist $A[p]$ ein Ideal von A, und $\{b\}$ ist wegen Vorbemerkung 2 für jedes $b \in A[p]$ ein endlicher Unterring von A. Da $A[p]$ im Fall $A \neq 0$, $p^2A=0$ von Null verschieden ist, und der Unterring

$$\{b\} (\neq 0, A[p])$$

minimale Unterringe $(\neq 0)$ enthält, die entweder Körper, oder Zeroringe, alle von Primzahlordnung sind, so hat jeder endlich erzeugbare nichttriviale Unterring von A im Falle $p^2A=0$ gewiß die Ordnung p.

Wir beweisen, daß jeder Ω-Ring mit $p^2A=0$ endlich ist. Gilt $pA \neq 0$, so ist Rang $(A[p])=1$, denn die endlich erzeugbaren Unterringe S von $A[p]$ sind, wie es in vorigen gezeigt wurde, von der Ordnung p. Dann gilt aber auch Rang $A^+=1$, woraus

$$A=\{a\},\ p^2a=0,\ a^2=da (d \in I)$$

folgen. Also ist A^+ zyklisch. Gilt nun $pA=0$, d. h. $A[p]=A$, so ist A im Fall $A=\{a\}$ wegen Vorbemerkung 2 endlich, denn eine Potenz von a kann durch die niedrigeren Potenzen von a ausgedrückt werden. Gelten aber $pA=0$ und $A \neq \{a\}$ für jedes a, so folgt aus der Existenz von minimalen Unterringen $(\neq 0)$ in $\{a\}$ sofort $|\{a\}|=p$. Es gibt also zu jedem Paar von Elementen $a \neq 0$, $b \neq 0$ mit $b \notin \{a\}$ ganze rationale Zahlen n_1, n_2, n_3 derart, daß

$$(a+b)^2=n_1(a+b),\ a^2=n_2a,\ b^2=n_3b$$

bestehen. Die Endlichkeit von $\{a, b\}$ folgt nun aus

$$ba=(n_1-n_2)a+(n_1-n_3)b-ab.$$

Da aber im Falle $\{a, b\} \neq A$ die Unterringe $\{a, b\}$ und $\{a\}$ beide von Primzahlordnung wären, was wegen $b \notin \{a\}$ unmöglich ist, gilt gewiß $\{a, b\}=A$. Also ist A endlich. Unser Satz in [5] bestimmt ganz explizit alle Ringe, deren alle echte Unterringe zyklische additive Gruppen besitzen. Da die additive Gruppe von jedem echten Unterringe des endlichen Ω-Ringes A nach den vorigen die Ordnung p hat, so kann der Satz in [5] angewendet werden. Hiernach hat jeder Ω-Ring $A(\neq 0)$ mit $pA=0$ die Mächtigkeit $|A|=p^q, p^2$ oder p. (Hierbei sind p und q beliebige Primzahlen.)

Im Fall $|A|=p$ ist A^+ offenbar zyklisch.

In weiteren genügt es nur den Fall $pA=0$ unterzusuchen, denn im Fall $pA \neq 0$, $p^2A=0$ ist A^+ zyklisch.

Ist der endliche Ω-Ring $A(\neq 0)$ mit $pA=0$ und $|A| \neq p$ halbeinfach, so folgt aus dem Wedderburn—Artinschen Struktursatz und der Definition des Ω-Ringes entweder $A \sim K_p \oplus K_p$ mit einem endlichen Primkörper K_p, oder $A \sim K$ mit einem endlichen Körper K von der Ordnung p^q, wobei p und q beliebige Primzahlen sind.

Ist zum Schluß der endliche Ω-Ring A mit $pA = 0$ und $|A| \neq p$ kein halbeinfacher Ring, so ist A wegen Vorbemerkung 3 gewiß nilpotent, und nach [5] folgt sofort $|A| = p^2$. Wir unterscheiden wiederum zwei Fälle.

Kann A mit $pA = 0$, $|A| = p^2$, $A^n = 0$ durch ein Element nicht erzeugt werden, so gilt $A = \{a, b\}$ mit

$$a^2 = pa = b^2 = pb = \{a\} \cap \{b\} = 0.$$

Hiernach ergibt sich $ab = l_1 a + l_2 b (l_i \in I)$, woraus auch

$$0 = ab^2 = l_1 ab = l_1^2 a + l_1 l_2 b, \quad l_1^2 a = -l_1 l_2 b \in \{a\} \cap \{b\}$$

folgen. Daher ist $p | l_1$ und ganz ähnlich auch $p | l_2$. Also gilt $ab = 0$. Ähnlich gewinnen wir auch $ba = 0$, folglich $A^2 = 0$.

Läßt sich aber A durch ein Element $a \in A$ erzeugen, gelten ferner $A = \{a\}$, $|A| = p^2$, $pa = a^n = 0$ $(a^{n-1} \neq 0,\ n \geq 2,\ n \in I)$, so erhält man $a^3 = m_1 a + m_2 a^2$ mit $m_i \in I$. Unser Zweck ist nun $a^3 = 0$ zu beweisen. Im Fall $a^3 = 0$ ist wegen $|A| = p^2$ gewiß $a^2 \neq 0$.

Wäre $(p, m_1) = 1$, so gäbe es eine Zahl n_1 mit

$$m_1 n_1 \equiv 1 \pmod{p} \quad (n_1 \in I),$$

woraus man mit der Bezeichnung

$$b = n_1(a^2 - m_2 a) \quad (\in \{a\})$$

eine Gleichung $a = ab$ erhält. Daher gilt aber auch

$$a = ab = ab^2 = \cdots = ab^{n-1} \in \{a\}^n = A^n = 0,$$

was wegen $a \neq 0$ unmöglich ist. Also ergibt sich $p | m_1$ und $a^3 = m_2 a^2$.

Im Fall $(p, m_2) = 1$ kann auch die Kongruenz

$$m_2 \cdot n_2 \equiv 1 \pmod{p} \quad (n_2 \in I)$$

gelöst werden. Dann ist $a^2 = a^2(n_2 a)$, woraus wegen $a^n = 0$ offenbar $a^2 = \cdots = a^2(n_2 a)^n = 0$ folgt, was der Voraussetzung $|A| = p^2$ widerspricht.

Also ist im Fall $A = \{a\}$, $|A| = p^2$, $pa = a^n = 0$ $(a^{n-1} \neq 0)$ gewiß $a^3 = 0$, w. z. b. w. Damit haben wir den Satz bewiesen.

Literaturverzeichnis

[1] L. Fuchs, *Abelian groups* (Budapest, 1958).
[2] N. Jacobson, *Structure of rings* (Providence, 1956).
[3] L. Rédei, *Algebra I* (Leipzig, 1959).
[4] L. Rédei—T. Szele, Die Ringe ersten Ranges, *Acta Sci. Math.*, **12** (1960), 18—29.
[5] F. Szász, Les anneaux ne contenant que des sous-anneaux propres cycliques, *Czechoslovak Math. J.*, **7** (82) (1957), 21—25.

(Eingegangen am 26. Mai 1960)